Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

James E. Cecchi (*pro hac vice forthcoming*)
Caroline F. Bartlett (*pro hac vice forthcoming*)
Jason M. Alperstein (*pro hac vice forthcoming*)
Kevin G. Cooper (*pro hac vice forthcoming*)
Jordan M. Steele (*pro hac vice forthcoming*)
CARELLA BYRNE CECCHI
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com
cbartlett@carellabyrne.com
kcooper@carellabyrne.com
jsteele@carellabyrne.com

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

DENISE FAIVRE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

PERRY JOHNSON & ASSOCIATES, INC., NORTHWELL HEALTH, INC. and COOK COUNTY HEALTH,

Defendants.

Case No. 2:23-cv-1926

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Denise Faivre ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this action against Perry Johnson & Associates, Inc. ("PJ&A"), Northwell Health ("Northwell"), and Cook County Health ("CCH", and together

"Defendants"), and alleges the following upon personal knowledge as to her own action and the investigation of her counsel, and upon information and belief as to all other matters, states as follows:

NATURE OF THE ACTION

1. Consumers trust doctors and healthcare service providers with protecting highly sensitive personal, financial, and medical information. Disclosure of such information may have a devastating impact on the lives of current and former patients, becoming the target of financial crimes, having their personal lives exposed, and intimate details of their medical treatments and conditions broadcasted to nefarious actors. The harm is palpable and irreversible. This action concerns the unlawful disclosure of patient information as the result of a data breach at PJ&A—a healthcare service provider—that provides transcription services to healthcare organizations and physicians for dictating and transcribing patient notes for hospital groups nationwide. Northwell, CCH, and other healthcare providers negligently or recklessly provided the healthcare information of their patients to PJ&A.

2. On November 3, 2023, Defendants revealed that hackers were able to obtain personal information such as: name, date of birth, address, medical record number, hospital account number, and clinical information such as the name of the treatment facility, the name of healthcare providers, admission diagnosis, date(s) and time(s) of service, and files containing transcripts of operative reports, consult reports, history and physical exams, discharge summaries or progress notes, which may include the reason for a patient's visit, their diagnoses, laboratory and diagnostic testing results, medical history including family medical history, surgical history, social history, medications, allergies, and/or other observational information (the "Data Breach").

3. In individual notification letters mailed to affected patients on or about November 3, 2023, PJ&A stated it first detected malicious activity by a third-party on May 2, 2023. This third-party gained access on March 27, 2023 and continued to have access to patient data for nearly *five weeks*, until May 2, 2023, and specifically for Northwell between April 7, 2023 and April 19, 2023. On June 21, 2023, PJ&A notified Northwell of the Data Breach. Notification of the Data Breach was inexplicably delayed *for over six months* while Plaintiff's and Class

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

Members (defined below) continued to be at risk for abuse by nefarious actors.

4. As a result of Defendants' actions and/or failure to act, Plaintiff and the Class experienced damages from: (i) theft of their personally-identifiable information ("PII") and protected healthcare information ("PHI") and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII and PHI; (iii) loss of value of their PII and PHI; (iv) the amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures; (v) Defendants' retention of profits attributable to Plaintiff's and other customers' PII and PHI that Defendants failed to adequately protect; (vi) economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiff is now exposed to; and (vii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this Data Breach.

JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 (d)(2). If a class is certified in this action, the amount in controversy will exceed $5,000,000.00, exclusive of interest and costs. There are more than 100 members in the proposed class, and at least one member of the proposed class is a citizen of a state different from Defendants.

6. This Court has personal jurisdiction over Defendants because the tortious harm inflicted on Plaintiff and the Class occurred from PJ&A's headquarters in Henderson, Nevada. Defendants also conduct and registered to do business in the State of Nevada, purposefully direct or directed their actions towards Nevada, and/or have the requisite minimum contacts with Nevada necessary to permit the Court to exercise jurisdiction.

7. Venue is also proper within this District because, pursuant to 28 U.S.C. § 1391(b)(2), Defendant PJ&A is headquartered in this District, maintained and stored the stolen data in this District, and a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated in this District. Northwell and CCH permitted Class Members' data to be transmitted, stored, and stolen in this District. Defendants' conduct caused harm to thousands of Class members residing in Nevada.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

PARTIES

8. Plaintiff Denise Faivre ("Plaintiff") has been a patient of Northwell since April 2017 and still receives its healthcare services. On November 3, 2023, Plaintiff received a letter from PJ&A informing her that an unauthorized party was able to access files stored on its computer network. Plaintiff was informed that this information potentially included her name, date of birth, address, medical record number, hospital account number, and clinical information such as the name of the treatment facility, the name of healthcare providers, admission diagnosis, date(s) and time(s) of service, and files containing transcripts of operative reports, consult reports, history and physical exams, discharge summaries or progress notes, which may include the reason for a patient's visit, their diagnoses, laboratory and diagnostic testing results, medical history including family medical history, surgical history, social history, medications, allergies, and/or other observational information.

9. Plaintiff is highly concerned, not only for herself, but also for her family. Many of Plaintiff's family members were affected by the breach including her: daughter, son, daughter-in-law, four grandchildren, brother, sister-in-law, and potentially others.

10. Since the Data Breach occurred, Plaintiff received a charge on her Discover credit card for a Netflix subscription, which she is not subscribed to. As a result, Plaintiff was forced to call Discover, dispute the charge, and request a new credit card. Plaintiff also registered for IdentityWorks, account monitoring, with Experian on or around November 15, 2023. Plaintiff also froze her credit reports, including on Experian, Equifax and TransUnion. Plaintiff has also spent time monitoring her accounts, discussing the Data Breach with her family, and protecting herself. Plaintiff is very concerned about identity theft and the consequences of such theft and fraud resulting from the data breach. Plaintiff places significant value in the security of her PII and PHI.

11. Defendant Perry Johnson & Associates, Inc. ("PJ&A") is incorporated in the state of Delaware with its principal place of business in Nevada. Defendant provides transcription services to healthcare organizations and physicians for dictating and transcribing patient notes for hospital groups nationwide.

12. Defendant Northwell Health ("Northwell") is headquartered in New Hyde Park, New York and is a nonprofit integrated healthcare network that is New York State's largest healthcare provider and private employer, with more than 81,000 employees.

13. Defendant Cook County Health ("CCH") is headquartered in Chicago, Illinois and is a nonprofit integrated healthcare network, and provides care to more than 500,000 individuals through the health system and the health plan.

FACTUAL BACKGROUND

The Data Breach

14. On November 3, 2023, Defendants announced the Data Breach in letters sent to affected patients. Defendants confirmed that hackers accessed the personal data of millions of patients. In a letter sent to those affected, PJ&A stated in relevant part as follows:

> **Perry Johnson & Associates. Inc.** ("PJ&A.," "we," or "us") is providing this letter to inform you of an event that may affect your personal health information. This letter provides details of the event, our response, and resources available to you to help protect your personal health information from possible misuse, should you feel it is appropriate to do so.
>
> **Who Is PJ&A and Why Did We Have Your Information?** PJ&A serves as a vendor to Northwell Health, Inc. and its subsidiaries and affiliates (collectively, "Northwell"). PJ&A provides certain transcription and dictation services to Northwell. In order to perform these services, PJ&A receives personal health information regarding
>
> **What Happened.** PJ&A became aware of a data security incident impacting our systems on May 2, 2023. We immediately initiated an investigation and engaged a cybersecurity vendor to further provide support in connection with our

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

investigation and secure against potential system vulnerabilities.

We promptly implemented the cybersecurity vendor-recommended actions to prevent the further disclosure of data as we continued to investigate the situation. Through our investigation, we determined that the unauthonzed access to our systems occurred between March 27, 2023 and May 2, 2023, and the unauthorized access to Northwell, patient data specifically occurred between April 7, 2023 and April 19. 2023.

On July 21, 2023. PJ&A notified Northwell that an unauthorized party had accessed and downloaded certain files from our systems. PJ&A had preliminarily determined that Northwell data was impacted on May 22, 2023 and by September 28. 2023. confirmed the scope of the Northwell data impacted.

What Information Was Involved. We have confirmed that certain files containing your personal health information were impacted by this incident. Specifically, the following information may have been impacted: your name, date of birth, address, medical record number, hospital account number, and clinical information such as the name of the treatment facility, the name of your healthcare providers, admission diagnosis, date(s) and time(s) of service, and files containing transcripts of operative reports, consult reports, history and physical exams, discharge summaries or progress notes, which may include the reason for your visit, your diagnoses. laboratory and diagnostic testing results, medical history including family medical history, surgical history, social history. medications, allergies. and/or other observational information.

What We Are Doing. We are committed to maintaining the privacy and security

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

> of your information and take this incident very seriously. PJ&A took, and will continue to take, appropriate steps to address this incident. including updating our systems to prevent incidents of this nature from occurring in the future.

15. Defendants stated it first detected malicious activity by a third-party on May 2, 2023. This third-party gained access on March 27, 2023 and continued to have access to patient data for nearly *five weeks*, until May 2, 2023. Defendants then waited over six months to inform Plaintiff and the Class, during which they may have been taking actions to defend themselves from malicious actors.

16. Defendant store massive amounts of sensitive personal and medical information, and should have had robust protections and monitoring in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files.

17. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII and PHI and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individual patients as a result of a breach.

Consequences of the Data Breach for Patients

18. Plaintiff and the Class have suffered actual harm and will continue to be harmed as a result of Defendants' conduct. Defendants failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. This breach may allow hackers to access the PII and PHI for Plaintiff and the Class. This PII and PHI may be publicly leaked online, which may allow for digital and potential physical attacks against Plaintiff and the Class. Now that the PII and PHI has been hacked, it is available for other parties to sell or trade and will continue to be at risk for the indefinite future.

19. Defendants' failure to keep Plaintiff's and Class Members' PII and PHI secure has severe ramifications. Given the sensitive nature of the PII and PHI stolen in the Data Breach – names, addresses, zip codes, phone numbers, email addresses, dates of birth, and Social Security numbers – hackers can commit identity theft, financial fraud, and other identity-related fraud

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff has suffered injury and faces an imminent and substantial risk of further injury, including identity theft and related cybercrimes due to the Data Breach.

20. Plaintiff's stolen PII and PHI may now be circulating on the dark web and it is highly valuable. Malicious actors use PII and PHI to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII and PHI to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create synthetic identities.

21. Further, malicious actors often wait months or years to use the PII and PHI obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII and PHI, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact that the Data Breach centralizes the PII and PHI and identifies the victims as Defendants' current, former, or prospective customers materially increases the risk to Plaintiff and the Class.

22. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[1] Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and PHI and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII and PHI obtained in the Data Breach is not used to harm them. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense

[1] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at: https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07- 737/html/GAOREPORTS-GAO-07-737.htm (last accessed: Nov. 20, 2023).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach. In other words, Plaintiff have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Breach.

23. Given Defendants' failure to protect Plaintiff's and the Class Members' PII and PHI despite multiple data breaches in the past as well as subsequent data breaches, Plaintiff have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII and PHI remains in Defendants' possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public as well as a large class of persons.

24. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and PHI and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII and PHI; (iii) loss of value of their PII and PHI; (iv) the amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures; (v) Defendants' retention of profits attributable to Plaintiff's and other customers' PII and PHI that Defendants failed to adequately protect; (vi) economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiff is now exposed to; and (vii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach.

CLASS ACTION ALLEGATIONS

25. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Nationwide Class and a New York Sub-Class, defined as follows:

Nationwide Class

All persons in the United States whose PII and PHI was maintained on PJ&A's systems that were compromised as a result of the breach announced by Defendants

SJG STRANCH, JENNINGS & GARVEY PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com

on or around November 3, 2023.

New York Sub-Class

New York Sub-Class: All persons in the State of New York whose PII and PHI was maintained on PJ&A's systems that were compromised as a result of the breach announced by Defendants on or around November 3, 2023.

26. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

27. There are numerous questions of law and fact common to Plaintiff and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants owed Plaintiff and other Class Members a duty to implement and maintain reasonable security procedures and practices to protect their PII and PHI, and whether it breached that duty;

a. Whether Defendants continue to breach duties to Plaintiff and other Class Members;

b. Whether Defendants' data security systems before the data breach met industry and other standards;

c. Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient way possible and without unreasonable delay;

d. Whether Plaintiff and other Class Members' PII and PHI was compromised in the data breach; and

e. Whether Plaintiff and other Class Members were damaged and will continue to be damaged as a result of Defendants' conduct.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

28. Plaintiff's claims are typical of the Class's claims. Plaintiff suffered the same injury as Class Members—*i.e.*, Plaintiff's PII and PHI was compromised in the Data Breach.

29. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor her counsel has interests that conflict with those of the proposed Classes.

30. Defendants have engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and other Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

31. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims.

32. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS
COUNT 1

NEGLIGENCE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

33. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-32 as if fully set forth herein.

34. Defendants collected sensitive PII and PHI from Plaintiff and Class Members when using Defendants' services or when that information was transmitted for processing.

35. Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and Class Members' PII and PHI in Defendants' possession was adequately secured and protected; (b) implementing processes that would detect a breach of their security systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry and other standards.

36. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described herein.

37. Defendants had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by Defendants' failure to protect their PII and PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

38. Defendants' duty to use reasonable security measures also arose as a result of the

special relationship that existed between Defendants, on the one hand, and Plaintiff and Class Members, on the other. The special relationship arose because Plaintiff and Class Members entrusted Defendants with their PII and PHI. Defendants alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

39. Defendants' duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII and PHI by companies such as Defendants. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTC Act that also create such a duty.

40. Defendants' duty also arose from Defendants' unique position as a large healthcare services provider in the United States. As a healthcare services provider, Defendants holds itself out as a protector of consumer data, and thereby assumes a duty to reasonably protect the data that was provided to it by Plaintiff and Class Members.

41. Defendants knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PII and PHI.

42. Defendants also had a duty to safeguard the PII and PHI of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require Defendants to reasonably safeguard sensitive PII and PHI, as detailed herein.

43. Defendants also had a duty to timely and adequately notify affected persons. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendants' misconduct.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

44. Defendants breached the duties owed to Plaintiff and Class Members described above and thus was negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII and PHI of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry and other standards during the period of the Data Breach; (d) comply with regulations protecting the PII and PHI at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiff's and the Class Members' PII and PHI in Defendants' possession had been or was reasonably believed to have been stolen or compromised.

45. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

46. Defendants' failure to take proper security measures to protect the sensitive PII and PHI of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' PII and PHI.

47. Plaintiff and Class Members were foreseeable victims of Defendants' inadequate data security practices, and it was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

48. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured, will continue to be injured, and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating

fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; lost value of access to their PII and PHI permitted by Defendants; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT 2

NEGLIGENCE *PER SE*

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

49. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-32 as if fully set forth herein.

50. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Defendants of failing to use reasonable measures to protect PII and PHI.

51. FTC publications and orders also form the basis of Defendants' duty.

52. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Defendants, including, specifically the damages that would result to Plaintiff and Class Members.

53. In addition, under state data security statutes, Defendants had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII and PHI.

54. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

55. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

56. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

57. Defendants breached duties to Plaintiff and Class Members under the FTC Act and state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

58. Plaintiff and Class Members were foreseeable victims of Defendants' violations of the FTC Act and state data security statutes. Defendants knew or should have known that the failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' PII and PHI would cause damage to Plaintiff and Class Members.

59. But for Defendants' violation of the applicable laws and regulations, Plaintiff's and Class Members' PII and PHI would not have been accessed by unauthorized parties.

60. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Members have been injured, will continue to be injured, and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; lost value of access to their PII and PHI permitted by Defendants; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 3

BREACH OF CONFIDENCE

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

61. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-32 as if fully set forth herein.

62. Plaintiff and Class Members maintained a confidential relationship with Defendants whereby Defendants undertook a duty not to disclose to unauthorized parties the PII and PHI provided by Plaintiff and Class Members to Defendants to unauthorized third parties. Such PII and PHI was confidential and novel, highly personal and sensitive, and not generally known.

63. Defendants knew Plaintiff's and Class Members' PII and PHI was disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the PII and PHI they collected, stored, and maintained.

64. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' PII and PHI in violation of this understanding. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards to protect the PII and PHI in its possession and failed to comply with industry-standard data security practices.

65. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

66. But for Defendants' disclosure of Plaintiff's and Class Members' PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Breach was the direct and legal cause of the unauthorized disclosure of Plaintiff's and Class Members' PII and PHI to third parties, as well as the resulting damages.

67. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' PII and PHI. Defendants knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' PII and PHI had serious security vulnerabilities because Defendants failed to observe basic information security practices or correct known or readily discoverable security vulnerabilities.

68. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and Class Members have been injured, will continue to be injured, and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; lost value of access to their PII and PHI permitted by Defendants; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT 4

INVASION OF PRIVACY – INTRUSION UPON SECLUSION

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

69. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-32 as if fully set forth herein.

70. Plaintiff shared PII and PHI with Defendants that Plaintiff wanted to remain private and non-public.

71. Plaintiff reasonably expected that the PII and PHI they shared with Defendants would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

72. Defendants intentionally intruded into Plaintiff's and Class Members' seclusion in an unreasonable and highly offensive manner by disclosing without permission their PII and PHI, which involved their private concerns, to a third party who then sold their PII and PHI to other third-parties on the dark web.

73. By failing to keep Plaintiff's and Class Members' PII and PHI secure, and disclosing PII and PHI to unauthorized parties for unauthorized use, Defendants unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, *inter alia*:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII and PHI properly obtained for specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII and PHI from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII and PHI without consent.

74. The PII and PHI that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII and PHI.

75. Defendants' intrusions into Plaintiff's and Class Members' seclusion were

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

76. As a direct and proximate result of Defendants' invasions of privacy, Plaintiff and Class Members have been injured, will continue to be injured, and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII and PHI; lost value of access to their PII and PHI permitted by Defendants; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Defendants' Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 5

UNJUST ENRICHMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

77. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-32 as if fully set forth herein.

78. In the alternative to the claims set out above, Defendants have been unjustly enriched as a result of the conduct described herein.

79. Plaintiff and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conferred upon, collected by, and maintained by Defendants and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

that was ultimately stolen in the Defendants Data Breach.

80. Defendants was benefitted by the conferral upon it of the PII and PHI pertaining to Plaintiff and Class Members and by its ability to retain, use, sell, and profit from that information. Defendants understood that it was in fact so benefitted.

81. Defendants also understood and appreciated that the PII and PHI pertaining to Plaintiff and Class Members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that PII and PHI.

82. But for Defendants' willingness and commitment to maintain its privacy and confidentiality, that PII and PHI would not have been transferred to and entrusted with Defendants.

83. Because of its use of Plaintiff's and Class Members' PII and PHI, Defendants sold more services and products than it otherwise would have. Defendants was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

84. Defendants also benefitted through the unjust conduct by retaining money that should have been used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII and PHI.

85. Defendants also benefitted through the unjust conduct in the form of the profits gained through the use of Plaintiff's and Class Members' PII and PHI.

86. It is inequitable for Defendants to retain these benefits.

87. As a result of Defendants' wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the PII and PHI belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the unauthorized disclosure of that PII and PHI), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

88. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Class Members' sensitive PII and PHI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

89. It is inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

90. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for Defendants to retain the benefit.

91. Defendants' defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and PHI and has caused the Plaintiff and Class Members other damages as described herein.

92. Plaintiff has no adequate remedy at law.

93. Defendants are therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of its wrongful conduct, including specifically: the value to Defendants of the PII and PHI that was stolen in the Data Breach; the profits Defendants received and is receiving from the use of that information; the amounts that Defendants overcharged Plaintiff and Class Members for use of Defendants' products and services; and the amounts that Defendants should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' PII and PHI.

COUNT 6

DECLARATORY JUDGMENT

On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Statewide Subclass

94. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-32 as if fully set forth herein.

95. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

96. An actual controversy has arisen in the wake of the Defendants Data Breach regarding their present and prospective common law and other duties to reasonably safeguard customers' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff continues to suffer injury as a result of the compromise of their PII and PHI and remain at imminent risk that further compromises of their PII and PHI will occur in the future given the publicity around the Data Breach and the nature and quantity of the PII and PHI stored by Defendants.

97. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure consumers' PII and PHI and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

98. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and other standards to protect consumers' PII and PHI.

99. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lacks an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries may not be readily quantified and he will be forced to bring multiple lawsuits to rectify the same conduct.

100. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs at Defendants, Plaintiff will likely be subjected to substantial identity theft and other damage. On

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

101. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff and Class Members demand judgment as follows:

A. Certification of the action as a Class Action under Federal Rule of Civil Procedure 23, and appointment of Plaintiff as a Class Representative and her counsel of record as Class Counsel;

B. That acts alleged above be adjudged and decreed to constitute negligence and violations of the laws of Nevada and any other applicable jurisdictions;

C. A judgment against Defendants for the damages sustained by Plaintiff and the Classes above, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

1. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors/penetration testers;
2. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;
3. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

4. Ordering that Defendants segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, unauthorized third parties cannot gain access to other portions of Defendants' systems;

5. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

6. Ordering that Defendants conduct regular database scanning and security checks; and

7. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. Awarding Plaintiff and Class Members prejudgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after service of this Complaint;

F. Disgorging Defendants of any amounts by which they were unjustly enriched;

G. Ordering Defendants to pay the costs of this suit, including reasonable attorney fees; and

H. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff, individually and on behalf of all those similarly situated, requests a jury trial, under Federal Rule of Civil Procedure 38, on all claims so triable.

DATED: November 20, 2023

Respectfully submitted,

/s/ Nathan R. Ring
Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, LLC
2100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102

James E. Cecchi (*pro hac vice forthcoming*)
Caroline F. Bartlett (*pro hac vice forthcoming*)
Jason M. Alperstein (*pro hac vice forthcoming*)

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Kevin G. Cooper (*pro hac vice forthcoming*)
Jordan M. Steele (*pro hac vice forthcoming*)
CARELLA BYRNE CECCHI
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com
cbartlett@carellabyrne.com
kcooper@carellabyrne.com
jsteele@carellabyrne.com

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC